



FOR IMMEDIATE RELEASE  
December 19, 2013

Contact: Doug Dunbar  
207-624-8525

## **State Officials Issue Consumer Protection Alert Following Data Breach Announcement by Target**

GARDINER – Governor Paul R. LePage joined officials at Maine’s Department of Professional and Financial Regulation to reassure consumers that state and federal laws are in place to protect them from major losses due to file breaches containing debit and credit card information, such as the one disclosed Thursday by Target.

“Although it’s unknown whether Maine consumers will be impacted by the Target data breach, I encourage people to closely monitor their credit and debit card statements, and to contact the financial institution that issued the card promptly if questionable charges appear,” Governor Paul R. LePage said. “Staff at Maine’s Department of Professional and Financial Regulation is also available to provide information and guidance.”

The Bureau of Financial Institutions and Bureau of Consumer Credit Protection at the Department of Professional and Financial Regulation outlined the following information and guidance for consumers responding to news of a financial data breach:

- Consumers should always thoroughly review credit and debit card statements from their bank or credit union.
- If a credit or debit card was used at a business that has experienced a data security breach, such as Target, or there is uncertainty about whether a card was used, consumers should be especially diligent in evaluating charges or withdrawals on their statement.
- Since the Target data breach reportedly began in November, consumers should review statements from November to the present.
- If consumers have online access to their credit or debit card information, they should review account activity as soon as possible, rather than waiting for the statement to arrive in the mail.
- If unknown charges or other suspicious activity appear on the account, consumers should notify the financial institution that issued the credit or debit card.
- Consumers do NOT need to contact the company that experienced the data breach, such as Target.

MORE

- Consumers' liability for unauthorized use of a CREDIT CARD is limited to \$50. If consumers report a loss to the credit card issuer before the credit card is used, the card issuer cannot hold consumers responsible for any unauthorized charges. If consumers have not lost the card itself, but the account numbers have been stolen, consumers have no liability for unauthorized use. Many cardholder agreements say that consumers are not responsible for any charges under any of these circumstances.
- Consumers noticing unauthorized activity on their DEBIT CARD resulting from a data breach have sixty (60) days from when the bank or credit union sent the statement to report it. If consumers fail to notify the bank or credit union of unauthorized transactions within this time, they are liable for the amount of the unauthorized transactions. This 60 day timeframe applies ONLY when the card's data has been compromised through a data breach, as in the Target case. See below for details about when a DEBIT CARD has been lost or stolen.
- When a DEBIT CARD has been lost or stolen, consumers have two (2) business days after learning of the loss or theft to notify their financial institution in order to limit their liability to \$50. If they do not notify their bank or credit union about the lost or stolen DEBIT CARD within two (2) business days, consumers may be liable for up to \$500 of the unauthorized transactions. If consumers do not notify their financial institution within sixty (60) days after being provided a monthly statement that lists a fraudulent debit, they can be liable for unauthorized withdrawals of any amount that occur after that 60 day period.
- To be safe, DEBIT CARD holders should act immediately if they notice unauthorized withdrawals.
- If impacted by unauthorized charges or withdrawals, consumers should first call the bank or credit union that issued the credit or debit card, and then follow up in writing to explain the problem.
- Some banks and credit unions may issue new cards to customers whose credit or debit card numbers are known to have been compromised through a data breach.
- Consumer may ask a financial institution to re-issue a new card if they have concerns about their account.
- Again, consumers do NOT need to contact the business that was subject to the data breach; and they need to contact the bank or credit union that issued their credit or debit card ONLY if they notice suspicious activity on their statement.
- For more information, contact the Bureau of Financial Institutions toll-free at 1-800-965-5235, or the Bureau of Consumer Credit Protection is 1-800-332-8529.

###